



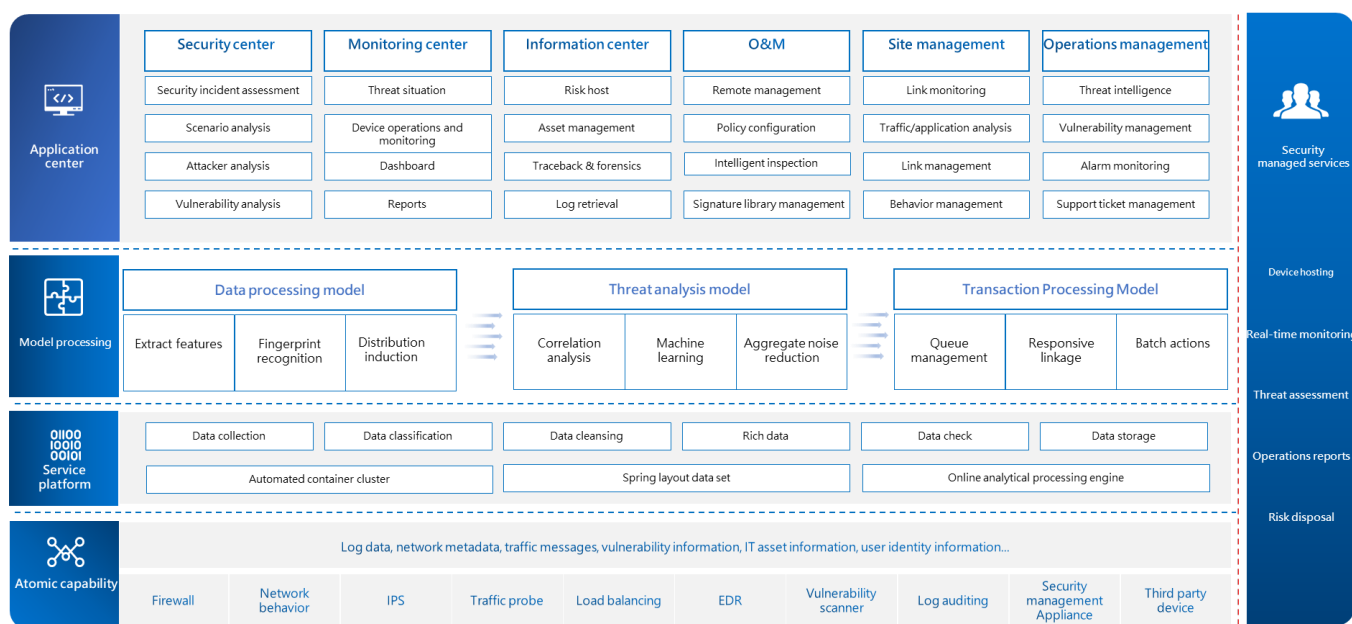
H3C SecCloud OMP Cloud O&M Platform

Release Date: Dec, 2024



Overview

H3C SecCloud OMP Cloud Operations Management Platform (OMP) is a Software as a Service (SaaS) solution developed by H3C for cloud-based security operations scenarios. It allows security devices to connect to the cloud with one click through a cloud channel, enabling real-time device status monitoring, configuration management, policy management, threat analysis, security situation presentation, and closed-loop incident handling. SecCloud OMP significantly reduces security device operation costs, shortens incident response times, swiftly identifies threat risks, and supports closed-loop decision-making by the security brain. SecCloud OMP helps enterprises rapidly and efficiently implement security capabilities.

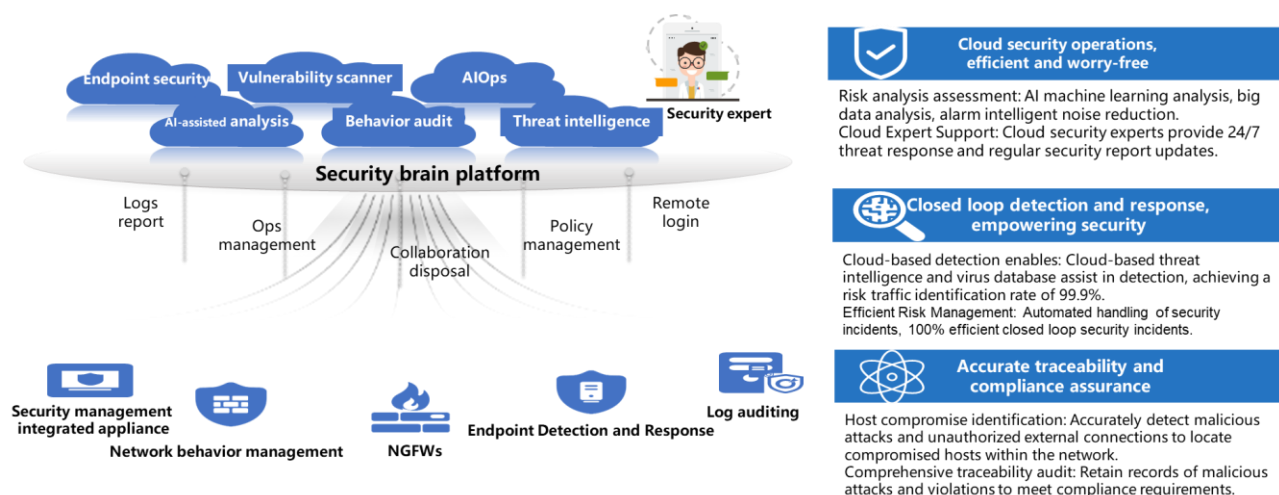


Capability architecture diagram for H3C SecCloud OMP

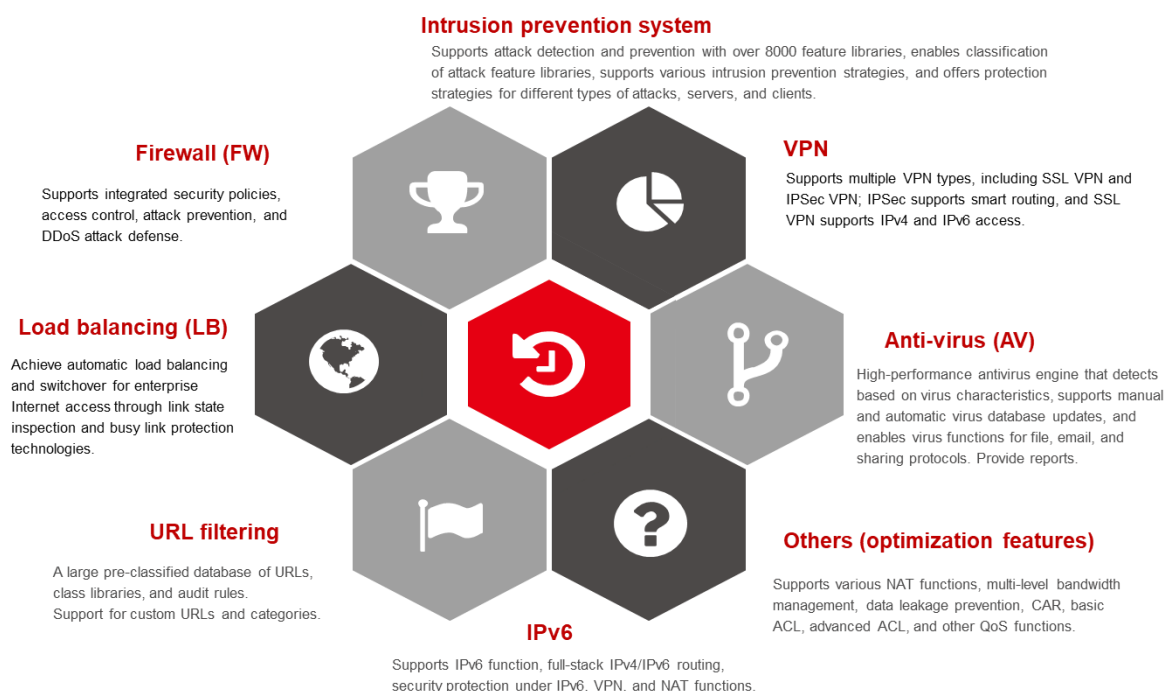
Features and benefits

Due to the increasing number of security devices acquired by enterprises with numerous branches and stores to meet security requirements, the workload for operations personnel has significantly increased. These enterprises encounter several challenges, such as insufficient operations capabilities among branch personnel, frequent network issues, and slow issue resolution. To address the operations issues related to security devices, H3C has launched SecCloud OMP. This platform allows security devices to connect to the cloud with one click through a

cloud channel. In the cloud, users can monitor device status in real-time, configure settings, and perform batch operations, significantly reducing operational time. SecCloud OMP provides various viewing and configuration methods, including Web and app interfaces, enabling you to identify and resolve issues anytime, anywhere, thus accelerating issue resolution. Combined with a cloud-based security situation analysis system, SecCloud OMP enhances the process of identifying, understanding, analyzing, and responding to security threats from a global perspective. Additionally, by integrating machine learning and artificial intelligence (AI), SecCloud OMP facilitates closed-loop decision-making by the security brain through intelligent analysis and coordinated responses, thereby implementing security capabilities.



Security component capabilities



Functions

One-click device access

SecCloud OMP allows security devices to connect to the cloud with one click through a cloud channel, ensuring seamless integration. This feature facilitates the automated deployment of configurations from the cloud to the devices. The operations personnel can monitor these security devices in real-time and gain prompt insights into their operational status. Moreover, operations personnel can perform automated security tasks on devices anytime, anywhere. This feature significantly reduces the complexity of individual configurations for customers and genuinely saves time. Comprehensive support for a rich variety of device types, including hardware firewalls, virtual machine firewalls, cloud firewalls, traffic probes, IPS, video firewalls, CPE gateways, internet behavior management, log auditing, and third-party devices, providing all-round security protection.

Convenient remote Ops

Moreover, operations personnel can perform automated security tasks on devices anytime, anywhere.

- **Deployment configuration:** Customers can customize deployment configuration on the cloud platform, which will be automatically deployed to the matching devices.
- **Reverse Web link:** SecCloud OMP allows customers to directly access the Web interface of a device for management operations.
- **Reverse CLI link:** SecCloud OMP also allows customers to directly operate a device remotely at its CLI.
- **Bulk configuration deployment:** From SecCloud OMP, customers can create device configuration templates and bulk deploy them to multiple devices by using the configuration management module, enabling efficient batch operations.

Unified and fine-grained configuration

SecCloud OMP with its unified management plane, supports unified management and configuration of configuration templates and also offers extensive options for fine-grained configuration management.

- **Unified management and configuration of configuration templates:** By specifying the applicable device models in a configuration template, you can enable different models of firewalls or application control gateways (ACGs) to share the same template, simplifying deployment.
- **Fine-grained configuration management:** Fine-grained configuration management supports the management of the following items: security policies, application security rules (IPS rules and AV rules), IPsec policies, objects, interfaces, VRFs, and security zones.

Massive multi-tenant management

SecCloud OMP supports a multi-tenant security architecture, which is widely applicable to public clouds, industry clouds, and private clouds. You can deploy one set of SecCloud OMP for use by multiple tenants in an organization, ensuring data isolation between tenants. SecCloud OMP supports managing over 100000 tenants, and supports the management of multiple tenants, roles, and sub-organization levels. SecCloud OMP ensures secure and isolated environments while delivering efficient and unified management, meeting diverse customer requirements.

AI empowerment, cloud-based protection

- **Top industry intelligence capability:** The cloud-based Threat Intelligence Center is updated in real-time, boasting a database of millions of malicious IPs, domains, URLs, and hundreds of millions of MD5 file threats.
- **AI-driven big data analysis:** By leveraging AI and machine learning technologies, SecCloud OMP performs in-depth analysis and evaluation of traffic, logs, and other information, achieving a detection rate of 99.9% while automatically generating security events. Perform targeted detection and identification for key malicious viruses such as mining and ransomware.

Accurate traceability, proactive threat management

- **Risky host tracing and identification:** Collect and screen risk information to generate a visualized security attack chain, making detailed tracing visible and easily locating the risky hosts.
- **Efficient closed-loop handling:** Match security threats in real-time, support one-click blocking to ensure the safety of the user's internal network environment.

Quality monitoring, intelligent VPN management

- **VPN link management:** Supports VPN encrypted connections for networking scenarios such as multiple branches in a headquarters. Supports intelligent VPN networking, automates IPsec VPN, SD-WAN, and VPN service route configuration and deployment.
- **Link quality monitoring:** It monitors the status of physical and VPN links, displaying latency, jitter, and packet loss metrics by region, and issues alerts for link anomalies.

Compliance audit, traffic behavior visibility

- **Overseas access auditing:** Provide compliance audits for overseas access traffic, supporting data monitoring and auditing based on access regions, domain names, external assets, and access trends.
- **Application traffic visibility:** Capture complete session information to display traffic distribution across sites, allowing you to trace specific traffic sessions, including IP, uplink/downlink, packet count, and user information.

Reporting

- **Security reports:** SecCloud OMP offers one-time security reports and periodic security reports for all organizational users. SecCloud OMP uses the security, audit, and other logs reported by the gateway to generate these reports based on the correlation rules, machine learning, threat intelligence, UEBA, and other threat

analysis models. The security report includes an overall security analysis and describes the organization's security management during the cycle from various dimensions such as security events, threat status, network conditions, and gateway conditions. It helps organizations understand past and ongoing threats and assists them in comprehending network security posture.

- **Inspection management:** Supports periodic intelligent inspection tasks, which monitor the status of security gateway devices, policy effectiveness, and alarm states, and generate standardized inspection reports to complete event notifications.

Cloud experts available 24 hours per day, 7 days per week

- **Expert analysis:** Cloud experts conduct real-time cybersecurity analysis, accurately handling events by collecting detailed threat information. They also provide precise notifications about risky host information, ensuring a complete closed-loop security event trace.

Standardized ticket management

The standardized ticket management feature of SecCloud OMP helps cloud administrators establish a standard and systematic cloud operations management process, ensuring efficient, fast, and orderly cloud operations services for cloud tenants.

- **Process-based function management:** Cloud tenants can request device maintenance services online, and the system administrator approves these requests and maintains devices online in the backend.
- **Process-based ticket Ops management:** Cloud tenants can submit tickets online, and the system administrator resolves issues in these tickets online in the backend.

One-stop Security SaaS Service

SecCloud OMP integrates a variety of advanced security value-added SaaS services, including cloud sandbox,

threat intelligence, situation awareness, and vulnerability scanning services. Tenants can choose and utilize the one-stop security services that best meet their unique security needs.

Multi-platform integration and convergence

SecCloud OMP seamlessly integrates with multiple platforms, such as H3C Oasis and U-Center, allowing users to manage security devices across various platforms, each with its own user interface. SecCloud OMP offers customized solutions tailored to different usage scenarios. You can enable integration with other platforms and data sharing with one click.

Typical deployments

SaaS deployment on public cloud

In public cloud Ops mode, the software and hardware components of SecCloud OMP are deployed on a public cloud platform to manage H3C security devices in the cloud environments or customer networks.

Deployment on private cloud

In industry-specific private cloud Ops mode, the software and hardware components of SecCloud OMP are deployed locally in the customer's data center to manage security devices across multiple branches of the customer's enterprise.

Ordering information

SecCloud OMP is a software-only product that requires a license certificate for use. Select licenses based on the number of security devices to be incorporated.

Product	BOM	Description	Notes
H3C SecCloud OMP License	3130A5WM	H3C SecCloud OMP-AI-NSQM1OMPAIPL - Security Brain Cloud Operation and Maintenance Platform Software License - Includes 100-node license	Required
SecCloud OMP 1-node License	3132A122	H3C SecCloud OMP-AI-NSQM1OMPAISN1 - Security Brain Cloud Operation and Maintenance Platform 1 Service Node Expansion License	Optional
SecCloud OMP 100-node License	3132A123	H3C SecCloud OMP-AI-NSQM1OMPAISN1H - Security Brain Cloud Operation and Maintenance Platform 100	Optional



The Leader in Digital Solutions

New H3C Technologies Co., Limited

Beijing Headquarters

Tower 1, LSH Center, 8 Guangshun South Street, Chaoyang

District, Beijing, China

Zip: 100102

Hangzhou Headquarters

Copyright ©2021 New H3C Technologies Co., Limited Reserves all rights

Disclaimer: Though H3C strives to provide accurate information in this document, we cannot guarantee that details do

not contain any technical error or printing error. Therefore, H3C cannot accept responsibility for any inaccuracy in this document.